servicenow

Now on Now: How Vendor Risk Management (VRM) enables us to complete risk assessments in less than half the time

VRM also helps us manage more assessments with no increase in staff.

Table of Contents

Introduction 2
What's at stake 2
The vendor risk assessment (VRA) process 3
Challenges 3
Our vendor risk journey 4
Phase 1 – Standardizing processes 4
Phase 2 – Integrating and automating workflows 4
Phase 2 Benefits 5
Phase 3 – Extending workflows 5
To learn more 6
About ServiceNow 6
Appendix 6
Our Customer Zero VRM team 6

Introduction

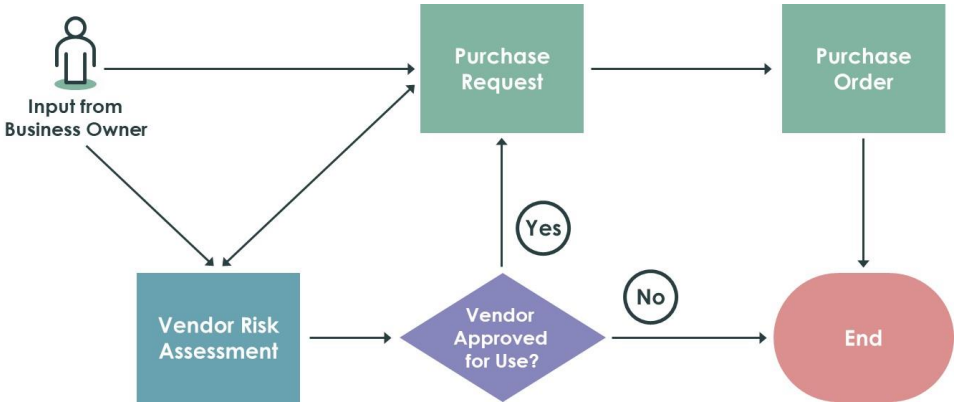
Vendors not only provide goods and services to ServiceNow, but many also play a role in delivering our solutions to employees and customers. And because vendors are part of the ServiceNow ecosystem, we must ensure that they have sufficient safeguards in place to prevent others from accessing our network through them, and then stealing our data or intellectual property—or that of our customers, partners or employees. That's why we assess each vendor, regardless of their size, prior to an engagement with ServiceNow.

What's at stake

A third-party breach can happen to any company. According to NormShield, in March 2020, major corporations from General Electric and T-Mobile to online giants like Amazon, eBay, and PayPal revealed that they had experienced a data breach caused by a third party.[1] This not only compromises the private data of the company, its employees, and customers, but can damage the company's operations and reputation. Breaches can also be costly. For example, GDPR fines can run into the tens of millions or even hundreds of millions of dollars for the largest companies, with fines up to 4% of global annual revenue or €20M, whichever is higher.

[1] NormShield, April 3, 2020

The vendor risk assessment (VRA) process



Our VRA team engages with vendors in two ways:

- The primary engagement is through a purchase request (PR) initiated by the business owner. Once a non-disclosure agreement has been sent to the vendor, a VRA ticket is created, and our assessment begins.
- We can also be engaged prior to a PR at the request of the business owner. This enables due diligence to take place prior to any purchasing activity.

We then send questionnaires to the vendor determine their relative risk in multiple areas, including security, web app security, anticorruption, and privacy. When the vendor returns the questionnaires, we review it for completeness and follow up as needed to fill any gaps.

Once we have completed our assessment, if the vendor is approved, we assign a risk level and add the information to the purchase request. A purchase order is then initiated. If the vendor is not approved, the process ends.

The VRA portion of the procurement process is then complete, however our work does not stop there. The VRA team collaborates with other teams, such as privacy, security, and legal to ensure that risks are addressed appropriately.

Challenges

Vendor risk assessment presents many challenges:

- **Everchanging legal and risk landscape** – Regulations are everchanging, especially around the handling of personal data, and can differ widely from region to region. It is incumbent upon VRA teams to stay on top of these changes—no small challenge, particularly for global companies.
- **Process variables** – Every vendor risk assessment is different; there is no one-size-fits-all approach. This requires both diligent and flexibility on the part of the VRA team.
- **Vendor data issues** – The information we receive from business owners and vendors is often flawed or insufficient. It often takes a lot of back-and-forth with the vendor to get all data issues resolved.

- **Labor-intensive process** – At many companies, including ServiceNow before we implemented ServiceNow® VRM, the process is very manual and labor-intensive. Multiple systems are involved, assessments are managed with spreadsheets, and coordination is done by email and phone.
- **Time pressure** – All of the above challenges can make the vendor onboarding process very time-consuming—and at times frustrating—for both ServiceNow and vendors, who are eager to begin their work.

Our vendor risk journey

The automation of workflows, aka digital transformation, is not a one-and-done effort, but an ongoing journey. Based on our own experience implementing VRM, we recommend a three-phased approach. This is effective, offers a fast path to value, and enables lessons learned to be applied in subsequent phases.

We formed a cross-functional team of subject matter experts to guide our journey and improve decision making (see appendix for details).

Phase 1 – Standardizing processes

We launched our third-party risk program by standardizing processes, particularly those that were inefficient and/or costly, and would generate near-term value. For example, creating standard vendor risk questionnaires generated immediate gains in efficiency. We also put a new due diligence process in place and established a central repository for assessments.

At the time we were using multiple systems—Governance, Risk, and Compliance (GRC) running on our internal instance of ServiceNow, and our procurement system—and tracking work manually in spreadsheets. We used this phase to tune our processes and identify areas for automation and improvement.

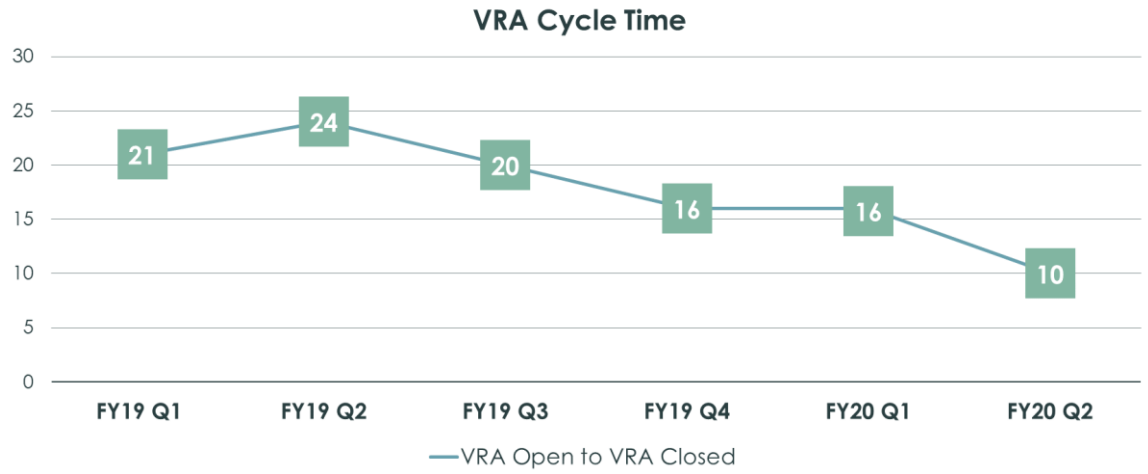
Phase 2 – Integrating and automating workflows

In this phase we moved off legacy systems to a single solution running on the Now Platform®. We implemented ServiceNow VRM and digitized and integrated processes to increase efficiency. For example, we automated notifications so that when a questionnaire was overdue, the system would send the vendor a reminder, thus offloading this routine administrative task from the VRA team.

We integrated Ariba with VRM, so that information would be pulled directly from Ariba into VRM, thereby eliminating a previous manual step.

We took advantage of the powerful analytic capabilities of the Now Platform. Dashboards let us see at a glance the status of every vendor assessment. They also streamlined and enhanced our reporting. Rather than having to gather and reconcile data manually, we drew upon the same dashboards we used in our daily work to build our reports, which increased data accuracy and management confidence.

Phase 2 Benefits



- **Greater visibility** – We can track each vendor's progress in completing a questionnaire and quickly answer any questions.
- **Faster assessments** – Automated workflows enable us to complete vendor risk assessments in less than half the time[2].
- **Increased productivity** – Since implementing VRM, we can process many more assessments with no increase in staff.
- **Reduced use of email** – Because vendor communication is managed by the system, email usage has dropped by 80%.
- **Enhanced experience** – Process improvements and automation have made work easier for the VRA team and provided a more efficient and professional experience for vendors.

Phase 3 – Extending workflows

Phase 3 will begin in 2021 and focus on integrating additional third-party tools to further enhance monitoring and program efficiency.

By this time, some vendor and supplier processes will be completely touchless. For example, Vendor Risk Management intake via the Tiering Assessment could then be automatically sent to the vendor, meaning that there is no human touch until the responses have been received. In addition, we will use the functionality of the system to automatically assess the risk levels in line with our company policies and processes.

We plan to take greater advantage of the growing capabilities of Performance Analytics, such as automated exporting of data.

We also will expand beyond security and privacy controls into areas such as financial risk and sustainability. This will paint a more holistic picture of our vendor risk.

[2] SID.Fac.92

To learn more

- Explore the ServiceNow Vendor Risk Management web page.
- Browse the Community forum for Governance, Risk, and Compliance to get tutorials and insights on a variety of risk-related topics. The New Vendor Risk Management Customers page offers step-by-step guidance to quickly lower your risk profile.

About ServiceNow

ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise. For more information, visit www.servicenow.com.

Now on Now is about how we use our own ServiceNow solutions to work faster, smarter, and better. With Now on Now, we're achieving true end-to-end digital transformation. To learn more, go to www.servicenow.com/nowonnow.

Appendix

Our Customer Zero VRM team

Before mapping out any digital transformation journey, it's helpful to have a cross-functional team of subject matter experts to optimize decision making and ensure that the solution benefits not only one group, but the enterprise as a whole.

As an example, our VRM Customer Zero team consists of the following:

- **Business** – The Vendor Risk Assessment team determines the functionality needed to meet the business need. As the industry experts, they also provide valuable feedback to the product team.
- **Product** – The product team develops the solution based on input from the VRA team and discussions with ServiceNow customers about the features they need in a VRM product.
- **Sales & Marketing** – Sales and Marketing are in constant contact with customers, assessing needs, monitoring trends, and honing messages about what the product is now and needs to be in the future.

- **IT Digital Business Services** – The IT team primarily supports the VRA team, but also plays an integral role in enabling communication among the other three parties.

# # #